Agenda

1. Review from Yesterday
2. Questions?
3. Today's Schedule

Review of Day 1

1. Why Perform a VA?
2. How a VA Works: Risk- and Performance-Based
3. What is your Mission?
4. What Threats Exist for your System?
5. What Level of Protection is Prudent?
6. What Consequences do you Want to Avoid?
7. What are your System's Vulnerabilities to the Threat you're Protecting Against?

Questions?

Today's Schedule

1. Types of Upgrades
2. Risk Matrix and Prioritization
3. Administrative Deadlines
4. Capital Improvement Plan
5. ERPs
6. Putting VAs and ERPs to Work for Improving Security

System Upgrades

Countermeasures to reduce risk fall into five categories

- Deterrence
- Detection
- Delay
- Response
- Recovery

V

C

Reduce Security Risks…

- Either by reducing C
  or
- By reducing V

Water systems generally cannot influence P

Reducing Risks

Improve Existing Protection System (V)

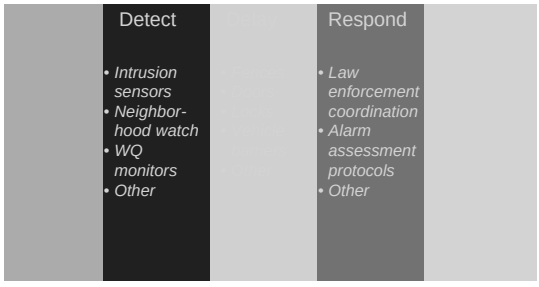
- **Deterrence**
- **Detection**
- **Delay**
- **Response (intercept attack)**

- **Reduce Consequences (C) to speed Recovery**
  - **Emergency Response**
  - **Redundancy**
  - **Resilience**

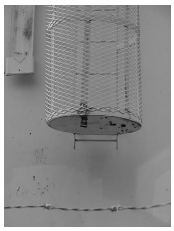
Reduce risks through a variety of approaches

Physical
Employee
Cyber
Knowledge
Customer

Classifying features by function helps identify needs



Reducing "V" at Finished Water Storage Facilities



Consider vulnerability to contamination and to physical damage

Possible Upgrades at a Storage Tank

- Electronic detection on tank hatch
- Baseline WQ monitoring
- Police surveillance
- Neighborhood watch
- Fence around tank with signage
- Closed circuit camera
- Hardened lock on access ladder
- Lights on area
- SOP for tank isolation
- SOP for security breach assessment

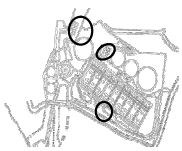
Risk Analysis and Upgrade Prioritization

How Do You Decide <u>What</u> Measures to Implement?

R = P x V x C where

- **R = Relative risk to critical asset**
- **P = Probability of a malicious act (threat)**
- **V = Vulnerability to a malicious act**
- **C = Consequences from a malicious act**

Risk equals…



P x V x C

Rating P, V, and C

- The following 3 slides are simply examples
- Define your own terms
- In this training, we consider only Low and High (L and H)
- Different methodologies use different rating systems
  - For example, RAM-W uses L, M, H

Probability: *How often might DBT strike?*

Very High:	Once a Year
High:	Every 1 – 5 Years
Moderate:	Every 6 – 10 Years
Low:	Every 10 or More Years

(In absence of specific threat against a facility, may set P = 1)

Vulnerability: *How unprotected are your facilities to DBT?*

- High: Virtually no countermeasures in place.
- Low: Reasonably strong protection countermeasures in place.

Consequences: *How serious is the incident?*

- **High – deaths, any illnesses, severe injuries, water loss to 30%+, regional economic impact**
- **Moderate – minor injuries, localized areas affected**
- **Low – water supply continues, or short interruptions**

Example: Risk of physical damage at a storage facility by a vandal DBT

- **Probability high – about once/year attacked by pranksters**
- **Vulnerability high – access is possible without detection**
- **Consequences low – vandal cannot inflict heavy damage on this particular facility**
- **Therefore, R = H*H*L**
- **How might this change if we consider vulnerability to contamination?**

Calculating relative risks

- **For simplicity, some VA methodologies drop P term (Presume P is same for all facilities of a system)**
- **For simplicity, we will drop P term**
- **The calculation is easier if you assign numbers to the ratings, such as**

  H=5

  L=1

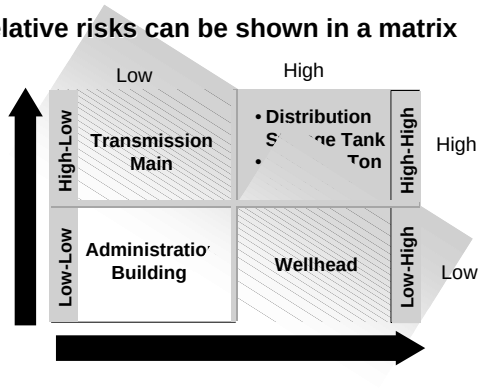
Exercise: Calculate relative risks at Water City

- For each asset , calculate R
- Rank the assets in order of highest to lowest risk
- Repeat the above steps for your own VA

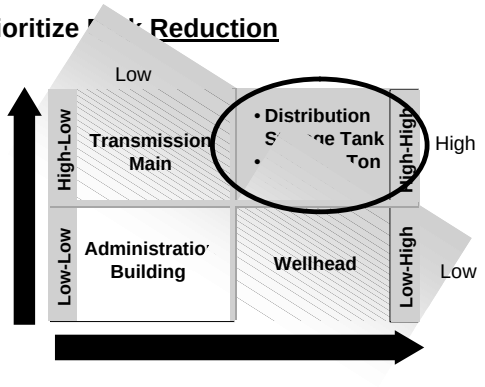
Prioritizing Improvements

- Can use matrix to aid in ranking risk reduction priorities
- Consider degree of risk reduction afforded by possible upgrades
- Can use matrix to aid in ranking costs and benefits

Relative risks can be shown in a matrix



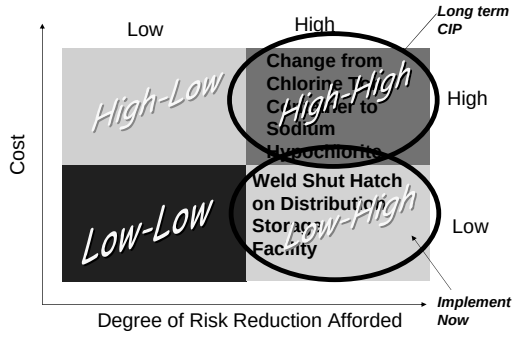
Prioritize Risk Reduction



Exercise: Water City's Priorities for Risk Reduction

- What items from Water City fall under the high-high risk category of the matrix?
- For each, identify risk reduction countermeasures (protection and recovery)
- Estimate degree of improvement afforded by the countermeasures identified for each asset (Would these countermeasures change the asset's overall risk R by lowering either V or C or both from H to L?)
- Repeat the above steps for your own VA

Prioritize Implementation



Exercise: Comparing Costs and Benefits of Security Upgrades

- Rate cost of countermeasure as L or H
- Rate degree of risk reduction as L or H (for example, if it reduces H*H to L*L, it affords a lot of risk reduction, so rate it as H)
- Identify any spinoff benefits (non-security-related) of the risk reduction measures
- Repeat the above steps for your own VA

Summary of risk assessment

- Can use matrix to aid in ranking risk reduction priorities
- Consider degree of risk reduction afforded by possible upgrades
- Can use matrix to aid in ranking costs and benefits

Next, Create an Action List for Acting on These Items…

Action Item List for VAs

- Rank security improvements by amount of risk reduction afforded
- Identify capital items (short, medium, long range improvements)
- Identify operational improvements
- Prepare CIP

Exercise: Putting Water City's VA into Action

- What low cost, high risk reduction countermeasures should be considered for immediate implementation?
- What high cost, high risk reduction countermeasures should be considered for inclusion in capital improvement plan (CIP)?
- Repeat the above steps for your own VA

Examples of Staff Roles in Security

Role	LEADERSHIP	IMPLEMENTATION	VIGILANCE	RESPONSE
MANAGEMENT				
OPERATIONS				
PLANNING AND ENGINEERING				
MAINTENANCE				
CUSTOMER SERVICE				

Additional Tools for Completing VAs

Additional Tools

- VSAT
  - http://www.vsatusers.net/ or 888-340-8830
  - ERP Format due in October, 2003
- RAM-W
  - Materials available through AWWARF
  - Sample VA available through AWWARF
- ASDWA-NRWA Checklists
- EPA Baseline Threat Information
- ISAC
- Cost info--EPA's product information ,etc.

Remember the Deadline:

June 30, 2004

VA Requirements for Small- to Mid-Sized Systems (3,301 to 49,999)

- Prepare and submit to EPA assessments of system vulnerability to terrorist attack
- Certify to EPA that an assessment was conducted
- Submit a written copy of VA to EPA
- Deadline: June 30, 2004

Emergency Response Plans (ERP)

What is an ERP?

- Plans, Procedures, Personnel, and Equipment that can:
  - Be utilized in the event of an intentional attack or natural disaster
  - Be utilized to avoid or significantly lessen the impact on public health of an attack or disaster

Relationship to VAs

- The VA considers threat scenarios and the likelihood of effective action
- The ERP and VA should be linked by consideration of the same threat scenarios, in addition to the natural disasters, accidents, and other emergencies already addressed in the contingency plan

Relationship to Current Contingency Plans

- Contingency Plans were developed to prepare for natural disasters, accidents, and emergencies but not security threats
- Must be supplemented with additional security-related scenarios to create a complete ERP

Top 10 Problems with ERPs

10. No one knew where the ERP was

- Decide in the beginning who the plan holders should be
- This decision will help dictate content
- Consider sensitivity of information, especially scenarios linked to VA
- Determine whether ERP should be placed on Intranet/ Internet
- Who responds to emergency initially—do they carry ERP around? Do they understand procedures?

9. ERP stayed on the shelf

- Consider who actually responds to emergencies in your organization
- Do front-line staff understand the plan and their own role in it?
- Do you make new staff aware of the plan?

8. ERP was too long

- Use checklists and diagrams
- Avoid verbosity

7. ERP was too short, with insufficient detail

- EAPs are important--Don't omit them!
- Do you have SOPs to supplement specifics?
- For example
  - Tank isolation procedures
  - Sketches of critical areas/ valves/ interconnects
  - Sampling protocols

6. ERP had flawed logic

- Coordinate plan with governing emergency management structure--county, state, federal
- Collaborate with other stakeholders (e.g., LEPC, MDEQ)

5. ERP presumed too much

- Include only currently existing resources
- Do not count on future facilities, agreements, or procedures
- Explain what the response would be if the situation occurred today

4. ERP used names of employees instead of staff positions in defining roles and responsibilities

- Corollary: Using staff position titles that are obsolete after reorganizing
- Every time someone is promoted or leaves the organization, ERP must be updated
- Using names throughout the document makes it more difficult to maintain

3. Phone numbers and other contact information were out of date

1. need to make this maintainable and assign responsibility for updates
2. Phone numbers and names scattered throughout document — not maintainable

2. ERP was written for the regulators, not for the water system

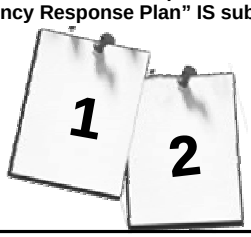
- ERP should be written around your needs
- Should be a document you WANT to consult during an emergency
- Organize it to reflect your system

1. ERP was never practiced

- First time everyone sees ERP should not be during an emergency
- Need to familiarize staff with plans and exercise them regularly

ERP Certification Submittals

- The Emergency Response Plan is NOT submitted to EPA
- The "Certification of Completion of an Emergency Response Plan" IS submitted – 2 pages



ERP Certification Submittals

For systems serving 3,000-50,000 population:

- Vulnerability Assessment is completed first and submitted to EPA (by June 30, 2004)
- Emergency Response Plans are due 6 Months after the VA is submitted (BEFORE December 30, 2004)

Applicable Laws

- State Regulations - Michigan Safe Drinking Water Act of 1976
- Federal Regulations - Public Health Security and Bioterrorism Preparedness and Response Act of 2002

Existing Contingency Plans in Michigan

- Part 23 of the Administrative Rules under the Michigan Safe Drinking Water Act (1976 PA 399)
- Effective Jan. 1978 for community water systems serving at least 200 individuals or 50 service connections

Contents of Existing Contingency Plans

- Program for rapid correction or mitigation of emergencies
- Copy of the water system general plan
- Description of the type, number, and capacity of standby power sources
- Listing of the duty assignments and schedule for updating the plan
- Listing of critical customers

Typical ERP Elements

1. Plan Activation, Roles and Responsibilities, and Command Structure
2. Internal Notifications, Contact Information, and Communications Technology
3. Public Notification and Media Communications
4. Mutual Aid Agreements, Emergency Procurement Guidelines
5. Staff Safety and Family Care
6. Specific Emergency Action Procedures

EPA's ERP Outline

I. Introduction – contents
II. Emergency Planning Process
III. Emergency Response Plan – Policies
IV. Emergency Action Procedures (EAPs)
V. Incident-Specific Emergency Action Procedures
VI. Next Steps – Plan review and approval, training
VII. Annexes – facility info
VIII. References and Links

EPA's ERP Outline

II. Emergency Planning Process
  - Planning Partnerships
  - Overall Emergency Management Structure
  - Scenarios

EPA's ERP Outline

III. **Emergency Response Plan - Policies**
- System Specific Information
- Identification of Alternate Water Sources
- Chain-of-Command Chart
- Communication Procedures
  - Internal notification
  - Local notification
  - External notification
  - Public/ media notification

EPA's ERP Outline

III. **Emergency Response Plan - Policies**
- Personnel Safety
- Equipment
- Property Protection
- Training, Exercises and Drills
- Assessment

EPA's ERP Outline

- Chain of Command
  - Emergency Manager (County Level Position)
  - Police and Fire Relationship
- Sampling
- Notification Procedures
  - Notifications Templates
  - Notification Lists

EPA's ERP Outline

IV. **Emergency Action Procedures**
- **Detailed procedures used in the event of an operational emergency or criminal act**

Emergency Action Procedures (EAPs)

- **Incident-specific response portion of an ERP**
- **Should address scenarios in the VA**
- **Procedures depend upon the incident**
- **Include the specifics - Who? What? Where? When?**
- **Documentation of what actions to take is important**

EPA's ERP Outline

v. **Incident-Specific Emergency Action Procedures**

NATURAL
- Tornado
- Storms
- Ice and snow
- Earthquakes

ACCIDENTS
- Fire
- Explosion
- Major Vehicle Accident
- Transportation Accident

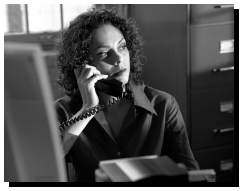
SUPPLY OUTAGE
- Electric power
- Water supply (resellers)
- Chemical suppliers

INDIVIDUAL CRIMINAL
- Disgruntled employee
- Vandalism
- Armed intruder
- Hacker

LARGE SCALE DISTURBANCE
- Riot
- Strike
- Bomb threat
- Terrorist threat
- Contamination event
- Organized computer attack
- Suspicious mail

Emergency Action Procedures (EAPs)

Example: Telephone Threat



- Protocol for handling telephone threats
- Forms to document threat information

Example: Contamination Incident

- Protocol for assessing credibility of incident and taking immediate action
- Sampling/ analysis protocol for unknown
- Procedures for immediate public notification
- Protocols for isolating tank, switching to alternative source, disposing of contaminated water

Example: SCADA System Failure

- Procedures for operating in manual control
- Protocol for call-back of staff
- Spare parts information
- Vendor support information

ERP Guidance Resources and Templates:

Are included in Section 5 of this guide

Other ERP Tools

- **State of Michigan Contingency Plan format**
- **EPA Response Protocol Toolbox (to be issued early 2004)**
- **Hydraulic Modeling Tools (under development)**
- **Expansion of Vulnerability Self-Assessment Tool for Water & WW (VSAT) - AMSA**

State Emergency Planning Committees

1986 Emergency Planning and Community Right-to-Know Act – Superfund

- **Required appointment of a State Emergency Planning Commission to address hazardous materials releases and other emergencies**
- **In Michigan, organized by Michigan State Police Emergency Management Division**

Local Emergency Planning Committees

- **State Emergency Planning Commission required establishment of Local Emergency Planning Committees in each county and some cities**
- **To date, 91 LEPCs formed**

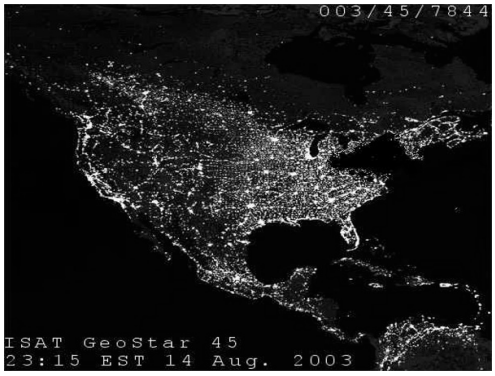
Local Emergency Planning Committee Info

- **EPA Database**
  - **www.epa.gov/ceppo/leplist.htm**
- **Michigan State Police**
  - **www.michigan.gov/msp/, Homeland Security**

Small Group Activity

- What EAPs should Water City include in its ERP?

THE BLACKOUT FROM SPACE – 8/14/03



Roundtable Discussion
Share Your Experiences!

- We Invite Everyone to Share Your Experiences During the Recent Power Outage With the Group
- Did Your ERP Work?
- If You Were Not Impacted, Do You Feel That Your ERP Would Provide Guidance During This Type of Situation?

Put Your ERP into Practice!

- Federal Emergency Management Agency (FEMA) Comprehensive Exercise Program defines 3 levels of exercise:
  1. Table-Top Exercise
  2. Functional Exercise
  3. Full Scale Exercise

Put Your ERP into Practice!

1. Table-Top Exercise
   - Introduce Scenario
   - Explain Implications On Functions
   - State Response
   - Done Prior to Functional Exercise

Put Your ERP into Practice!

2. Functional Exercise
   - Simulation in "Real Time"
   - Done in a Room With All Reps Involved
   - State/County Emergency Response Personnel Participate
   - Recommended on a Quarterly Basis

Put Your ERP into Practice!

3. **Full Scale Exercise**
   - **Simulations (Drills) But Acted Out in "Real Time"**
   - **All Representatives Available**
   - **State/County Emergency Response Personnel Participate**
   - **Some Hazard Drills Annually**
   - **Full Scale Exercise Frequency Dependent on Complexity**

Full-Scale Exercise TOPOFF2 – May 12, 2003

- **5-day full-scale mass destruction exercise (explosion of radioactive material)**
- **Chicago, District of Columbia, and Seattle Metro areas**
- **U.S. and Canadian government departments**
- **Dept. of Homeland Security (FEMA)**

Local Emergency Planning Committees & Water Utilities

- **Join your local LEPC**
- **If not possible to join, go to meetings and establish communications**
- **Take advantage of training:**
  - **Courses – Examples:**
    - **Basic Skills in Emergency Management**
    - **Disaster Response and Recovery Operations**
  - **Certification**

Local Emergency Planning Committees & Water Utilities

- Take advantage of training available through agencies:
- MICHIGAN HAZARDOUS MATERIALS TRAINING CENTER
  - Courses – Examples:
    - Basic Skills in Emergency Management
    - Disaster Response and Recovery Operations
  - Certification
- FEMA (DEPT. OF HOMELAND SECURITY)

Action Item List for ERPs

- Link to scenarios in VA
- Coordinate development with LEPC and other applicable plans
- Identify emergency action procedures
- Assign responsibility to maintain ERP

How do I implement?

Process + Plan = Protection

- **Continuous Improvement Process**

  integrated with a

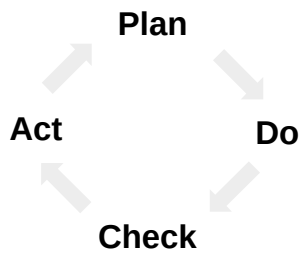
- **Capital Improvement Plan**

  will result in

- **Critical Infrastructure Protection**

CIP³

CIP³ - Continuous Improvement Process



CIP³ - Capital Improvement Plan

- Identify Funding
  - State Drinking Water Revolving Fund
  - Capital Improvement Fund
  - Bonds/Loans
  - Future Grants???
- Seek authorization
- Implement
- Establish an annual process

CIP^3 - Critical Infrastructure Protection

- A successful VA program will result in critical infrastructure protection if you:
  - PLAN - for a reasonable threat and prioritize vulnerabilities
  - DO – implement the prioritized projects
  - CHECK – that the implemented projects meet their goals and objectives
  - ACT – on changes to the system or threats in the future and continuously keep the ERP relevant and updated

In Summary:

- Vulnerability Assessment is a risk-based process
- R = P x V x C
- VA Tools are available
- Results from VA must be incorporated into the Emergency Response Plan and Capital Improvement Plan
- Compliance Deadlines are approaching

Web sites

- MDEQ -Water Division web site:

  http://www.michigan.gov/deq/0,1607,7-135-3313---,00.html

  Or

  http://www.michigan.gov/deq

  In the left column click on “Water”

  Then click on “Homeland Security”
- USEPA

  http://www.epa.gov/safewater/security/

Thank You!

- Questions?
  - MDEQ

    Robert F. Babcock
    Security and Emergency Response Coordinator
    Water Division
    517-373-8566
    babcockr@michigan.gov
  - CDM

    Mike Kovach
    KovachMP@cdm.com
    517-702-1213